Cassandra Crossing/ Apocalisse Bitcoin

(619)—La disponibilità di computer quantistici permetterà di rubare i bitcoin? E basteranno il Falco, la Sfinge ed il Cristallo di…

Cassandra Crossing/ Apocalisse Bitcoin



Figure 1:

(619)—La disponibilità di computer quantistici permetterà di rubare i bitcoin? E basteranno il Falco, la Sfinge ed il Cristallo di Dilitio a salvarci?

25 aprile 2025—I 24 instancabili lettori di Cassandra avranno certamente apprezzato l'esternazione sull'Apocalisse Quantistica prossima ventura.

Si tratta di un grido di allarme sulla **sottovalutazione di una vecchia questione**, ormai scesa sotto la soglia di attenzione dei più. In estrema sintesi, **tutta la crittografia che abbiamo utilizzato e stiamo utilizzando verrà resa violabile dai computer quantistici**, non appena questi ultimi diverranno disponibili.

Tutto (più o meno) potrà essere decrittato, violato, falsificato.

Ma detta così, in termini generali e totalizzanti, questa facile profezia non fa tutta la paura che dovrebbe. E per fare bene il proprio mestiere, la vostra profetessa preferita dovrà fare di più.

Proviamo quindi a restringere il campo, considerando una cosa sola, le criptovalute, ed in particolare il Bitcoin. Chi avesse bisogno di informazioni di base sul Bitcoin, potrebbe seguire questo breve corso.

Visto che le criptovalute sono "*fatte*" di crittografia, sono certamente a rischio. **Il Bitcoin** poi, che è la criptovaluta più "*antica*", e che è basato sullo stato dell'arte crittografica del 2009, **è praticamente spacciato**.

Adesso qualcuno tra i 24 informatissimi lettori dirà "*Ma in Bitcoin le chiavi non sono basate sulla fattorizzazione dei numeri primi, ma sulle molto più sicure curve ellittiche*".

Tutto vero, ma insufficiente. Gli algoritmi ED25519 e ECDSA, e gli altri algoritmi utilizzati da Bitcoin, sono più robusti degli onnipresenti RSA e DH, ma non sono comunque quantum-resistant; quindi la blockchain di Bitcoin potrà essere attaccata in una quantità di modi non appena qualcuno disporrà di adeguati computer quantistici.

Tralasciando altri attacchi possibili, come falsificare transazioni e corrompere la blockchain stessa, sarà certamente possibile "rubare" con semplicità una buona percentuale dei bitcoin esistenti.

Circa il 20% dei bitcoin in circolazione sono stati infatti "spesi" utilizzando più di una volta lo stesso indirizzo bitcoin. Questo fatto "espone" alcune informazioni, come la chiave pubblica del portafoglio, e rende quindi "semplice" calcolare la chiave privata (lo so, sembra un'eresia, ma è il potere dei quanti), ed impossessarsi di tutti i bitcoin del portafoglio che ha quella chiave.

Ma se impossessarsi del 20% dei bitcoin circolanti vi sembra poco, potete tranquillamente supporre che esistano molti altri tipi di attacchi quantistici agli algoritmi crittografici utilizzati meccanismi interni di Bitcoin. Certamente ci sono persone competenti che da tempo si stanno occupando di cercarli, e che ne avranno già preparati un bel po'.

Pensate cosa può significare calcolare la chiave privata di Satoshi Nakamoto, quella che firma la transazione della Genesi della blockchain, il mitico Blocco Zero. Aldilà di altre possibilità, che lasciamo all'immaginazione di persone molto più competenti di Cassandra, Satoshi Nakamoto possiede sulla blockchain più di **un milione di bitcoin, circa 100 miliardi di dollari**, vuoto per pieno.

E che dire dei 4 milioni di bitcoin che si stimano ormai "*indisponibili*" perché i loro proprietari si sono perse le chiavi private dei loro portafogli? Tentare di recuperarli e riconsegnarli ai loro disattenti proprietari potrebbe essere una buona azione per dei boy-scout dotati di computer quantistici. Ma anche tenerseli è altrettanto possibile

Al giorno d'oggi, i proprietari di un buon numero di Bitcoin sono certamente dei fortunati mortali. Se sono anche mediamente previdenti e stanno leggendo questo articolo, Cassandra si permette di suggerire di diversificare il loro patrimonio, magari verso investimenti certamente quantum-resistant, come i lingotti d'oro, il petrolio, la soia e tutti quei beni dotati di un robusto valore d'uso.

Infatti tutta la finanza, non solo quella delle criptovalute, rischia di uscire assai male dall'Apocalisse Quantistica.

"*Ma cosa c'entrano comunque i cristalli di Dilitio con l'apocalisse quantistica?*", dirà certamente uno dei 24 impazienti lettori.

I nuovi algoritmi dai nomi immaginifici, *Falco, Sfinge e Cristallo di Dilitio* son appunto i primi algoritmi crittografici post-quantistici che l'anno scorso il NIST ha rilasciato, per realizzare i nuovi sistemi crittografici immuni dalla apocalisse quantistica.

Purtroppo, anche solo introdurre piccole modifiche nel funzionamento di Bitcoin e nella sua blockchain richiede di ottenere il consenso di una cospicua maggioranza dei nodi, cosa difficilissima, come gli ultimi 16 anni di storia del Bitcoin hanno ben dimostrato.

Inoltre, cambiamenti di algoritmi di questa portata richiederebbero quello che viene chiamato "hard fork", e la creazione di una nuova blockchain. In questo caso si aprirebbe il problema della migrazione dei bitcoin dalla vecchia blockchain a quella nuova, cosa che richiederebbe la creazione di un protocollo di trasferimento e di un processo superaffidabile e supercondiviso per consentire questa operazione.

Sarebbe poi necessario che tutti i proprietari di wallet facessero manualmente l'operazione, cosa impossibile per circa il 20% dei bitcoin ormai indisponibili, e difficile per quelli le cui credenziali non siano conservate da un singolo individuo.

Inoltre all'inizio i "nuovi" bitcoin varrebbero poco, aumentando col tempo, mentre i vecchi bitcoin comincerebbero a perdere valore mano mano che il processo si realizza. I primi che accettassero di fare il trasferimento, dovrebbero fare un atto di fede, e cambiare una cosa che vale molto con una cosa che vale di meno.

Sarebbe perciò necessario creare un disincentivo a rimanere sulla vecchia blockchain, facendo in modo che i vecchi bitcoin ad un dato momento non fossero più scambiabili, tramite il blocco della vecchia blockchain, altrimenti l'incentivo al cambiamento sarebbe basso. Tutto molto, molto ma molto difficile.

E poi siamo sicuri che questo non stia già succedendo? Che qualcuno, già dotato di computer quantistici, stia pian piano rubando quello che appartiene a proprietari che non possono accorgersene perché spariti o distratti?

Bene, certamente non ancora. La blockchain di Bitcoin, ricordiamo, è completamente pubblica, e scrutinata in continuazione da molti attori.

Questo ne fa un ideale "canarino nella miniera" per l'avvento dei computer quantistici.

Nel momento in cui wallet fermi da molto tempo, come quelli di Nakamoto od altri definiti "indisponibili", dovessero ricominciare ad operare trasferendo cifre importanti, questo sarebbe un indizio molto forte dell'utilizzo occulto di computer quantistici da parte di attori importanti.

Forse, proprio per questo motivo, questi attori decideranno di fare ben altro, e ce ne accorgeremmo da rivolgimenti, catastrofi e guerre ben più importanti.

Posto che ci sia ancora tempo, e che l'apocalisse quantistica non provochi danni tali da minacciare la sopravvivenza della società tecnologica, introdurre gli algoritmi post-quantistici non solo nel Bitcoin ma in tutte le infrastrutture informatiche di oggi è una priorità assoluta.

La loro adozione non sarà mai troppo veloce.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on May 4, 2025.

Canonical link

Exported from Medium on August 27, 2025.